Cloud Security Engineer

Content

Module 1: Preparing for Your Professional Cloud Security Engineer Journey

- **Topics:**
  - Introduction
  - Configuring Access Within a Cloud Solution Environment
  - Ensuring Data Protection
  - Managing Operations in a Cloud Environment
  - Ensuring Compliance

Module 2: Google Cloud Fundamentals: Core Infrastructure

- **Topics:**
  - Introducing Google Cloud
  - Resources and Access in the Cloud
  - Virtual Machines and Networks in the Cloud
  - Storage in the Cloud
  - Containers in the Cloud
  - Applications in the Cloud
  - Developing and Deploying in the Cloud
  - Logging and Monitoring in the Cloud
- **Hands-On:**
  - A Tour of Google Cloud Hands-on Labs
  - Compute Engine: Qwik Start - Windows
  - Getting Started with Cloud Shell and gcloud
  - Kubernetes Engine: Qwik Start
  - Cloud Storage: Qwik Start - Cloud Console

Module 3: Networking in Google Cloud: Defining and Implementing Networks

- **Topics:**
  - Google Cloud VPC Networking Fundamentals
  - Controlling Access to VPC Networks
  - Sharing Networks Across Projects
  - Load Balancing
- **Hands-On:**
  - Multiple VPC Networks

    - VPC Network Peering
    - VPC Networks - Controlling Access
    - HTTP Load Balancer with Cloud Armor
    - Create an Internal Load Balancer

Module 4: Managing Security in Google Cloud

- **Topics:**
    - Foundations of Google Cloud Security
    - Cloud Identity
    - Identity and Access Management (IAM)
    - Configuring Virtual Private Cloud for Isolation and Security
- **Hands-On:**
    - Cloud IAM: Qwik Start
    - IAM Custom Roles
    - Service Accounts and Roles: Fundamentals
    - User Authentication: Identity-Aware Proxy
    - Getting Started with Cloud KMS
    - Setting up a Private Kubernetes Cluster

Module 5: Logging, Monitoring, and Observability in Google Cloud

- **Topics:**
    - Introduction to Monitoring in Google Cloud
    - Avoiding Customer Pain
    - Alerting Policies
    - Monitoring Critical Systems
    - Configuring Google Cloud Services for Observability
    - Advanced Logging and Analysis
    - Monitoring Network Security and Audit Logs
    - Managing Incidents
    - Investigating Application Performance Issues
    - Optimizing the Costs of Monitoring
- **Hands-On:**
    - Cloud Monitoring: Qwik Start

Module 6: Security Best Practices in Google Cloud

- **Topics:**
    - Securing Compute Engine: Techniques and Best Practices
    - Securing Cloud Data: Techniques and Best Practices
    - Application Security: Techniques and Best Practices
    - Securing Kubernetes: Techniques and Best Practices
- **Hands-On:**

- Migrating to GKE Containers
- How to Use a Network Policy on Google Kubernetes Engine
- Using Role-based Access Control in Kubernetes Engine
- Google Kubernetes Engine Security: Binary Authorization
- Securing Applications on Kubernetes Engine - Three Examples
- Hardening Default GKE Cluster Configurations

Module 7: Mitigating Security Vulnerabilities on Google Cloud Platform

- **Topics:**
  - Securing Compute Engine
  - Securing Cloud Data
  - Protecting Against Distributed Denial of Service (DDoS) Attacks
  - Application Security
  - Content-Related Vulnerabilities
- **Hands-On:**
  - Configuring, Using, and Auditing VM Service Accounts and Scopes
  - Using Customer-Managed Encryption Keys with Cloud Storage and Cloud KMS
  - Configuring Traffic Blocklisting with Google Cloud Armor
  - Using Web Security Scanner to Find Vulnerabilities in an App Engine Application